AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Original) In a station that is capable of communicating with at least one access point in a communications network, a method for creating a secure association between the station and at least one access point, the method comprising:

obtaining discovery information from one or more access points in the communications network, the discovery information reflecting capabilities of the one or more respective access points to facilitate communication with the station;

selecting one of the access points to become associated with;

authenticating the selected access point;

sending a discovery verification request to the selected access point for the discovery information of the selected access points to be verified; and

receiving an acknowledgement receipt from the selected access point verifying the discovery information.

2. (Original) A method as recited in claim 1, wherein the discovery verification request includes an identifiable security object obtained during authentication.

3. (Original) A method as recited in claim 2, wherein the identifiable security object includes at least one of an encryption key, a certificate and a hash number.

4. (Original) A method as recited in claim 1, wherein authenticating the access point includes identifying a certificate from a trusted certificate authority.

5. (Original) A method as recited in claim 4, wherein the trusted certificate authority is a server of the communications network

6. (Original) A method as recited in claim 1, wherein authenticating the access point is part of a mutual authentication that also involves the access point authenticating the station.

7. (Original) A method as recited in claim 1, further including an act of sending a frame to the access point after receiving the acknowledgment receipt, wherein the frame includes a verifiable key that indicates to the access point that the frame is actually received from the station.

8. (Original) A method as recited in claim 7, wherein the frame includes a management frame configured to control the secure association between the access point and the station.

9. (Original) A method as recited in claim 8, wherein the management frame is configured to terminate the secure association.

10. (Original) A computer program product for use in a station that is capable of communicating with at least one access point in a communications network, the computer program product comprising one or more computer-readable media having computer-executable instructions for implementing a method for creating a secure association between the station and at least one access point, the method comprising:

obtaining discovery information from one or more access points in the communications network, the discovery information reflecting capabilities of the one or more respective access points to facilitate communication with the station;

selecting one of the access points to become associated with;

authenticating the selected access point;

sending a discovery verification request to the selected access point for the discovery information of the selected access points to be verified; and

receiving an acknowledgement receipt from the selected access point verifying the discovery information.

11. (Original) A computer program product as recited in claim 10, wherein the discovery verification request includes an identifiable security object obtained during authentication.

12. (Original) A computer program product as recited in claim 11, wherein the identifiable security object includes at least one of an encryption key, a certificate and a hash number.

13. (Original) A computer program product as recited in claim 10, wherein authenticating the access point includes identifying a certificate from a trusted certificate authority.

14. (Original) A computer program product as recited in claim 13, wherein the trusted certificate authority is a server of the communications network

15. (Original) A computer program product as recited in claim 10, wherein authenticating the access point is part of a mutual authentication that also involves the access point authenticating the station.

16. (Original) A computer program product as recited in claim 10, wherein the method further includes an act of sending a frame to the access point after receiving the acknowledgment receipt, wherein the frame includes a verifiable key that indicates to the access point that the frame is actually received from the station.

17. (Original) A computer program product as recited in claim 16, wherein the frame includes a management frame configured to control the secure association between the access point and the station.

18. (Original) A computer program product as recited in claim 17, wherein the management frame is configured to terminate the secure association.

19. (Original) In an access point that is capable of communicating with at least one station in a communications network, a method for creating a secure association between the station and at least one access point, the method comprising:

providing discovery information to the station, the discovery information reflecting capabilities of the access point to facilitate communication with the station;

providing a certificate with the discovery information that is used by the station to authenticate the access point;

receiving a discovery verification request from the station for the discovery information to be verified; and

verifying the discovery verification request to the station.

20. (Original) A method as recited in claim 19, wherein the discovery verification request includes an identifiable security object obtained during authentication of the access point by the station.

21. (Original) A method as recited in claim 20, wherein the identifiable security object includes at least one of an encryption key, a certificate and a hash number.

22. (Original) A method as recited in claim 19, wherein the certificate is signed by a server of the communications network

23. (Original) A method as recited in claim 19, further including an act of authenticating the station as an authorized network device.

24. (Original) A computer program product for use in an access point that is capable of communicating with at least one station in a communications network, the computer program product comprising one or more computer-readable media having computer-executable instructions for implementing a method for creating a secure association between the station and at least one access point, the method comprising:

providing discovery information to the station, the discovery information reflecting capabilities of the access point to facilitate communication with the station;

providing a certificate with the discovery information that is used by the station to authenticate the access point;

receiving a discovery verification request from the station for the discovery information to be verified; and

verifying the discovery verification request to the station.

25. (Original) A computer program product as recited in claim 24, wherein the discovery verification request includes an identifiable security object obtained during authentication of the access point by the station.

26. (Original) A computer program product as recited in claim 25, wherein the identifiable security object includes at least one of an encryption key, a certificate and a hash number.

27. (Original) A computer program product as recited in claim 24, wherein the certificate is signed by a server of the communications network

28. (Original) A computer program product as recited in claim 24, the method further including an act of authenticating the station as an authorized network device.

29. (Currently Amended) In a first network device that is engaged in a secure association with a second network device in a communications network, a method for verifying management frames transmitted between the network devices, the method comprising:

at the first network device creating a management frame configured to control the secure association;

at the first network device attaching a verifiable key to the management frame, wherein the verifiable key is used to perform an integrity check;

and

at the first network device sending the management frame with the verifiable key to the second network device, wherein upon receiving the management frame and the verifiable key, the second network device recognizes the verifiable key and verifies the management frame prior to executing the management frame.

30. (Original) A method as recited in claim 29, wherein at least one of the first and second network devices is a station configured to access the network and wherein at least one of the first and second network devices is an access point configured to provide the station access to the communications network.

31. (Original) A method as recited in claim 30, wherein the first network device is a mobile and wireless communications device.

32. (Original) A method as recited in claim 29, wherein the verifiable key is a provided by a server of the communications network.

33. (Original) A method as recited in claim 29, wherein the verifiable key comprises a derivative of a key formed during authentication of at least one of the first and second network devices.

34. (Original) A method as recited in claim 29, wherein prior to sending the management frame, the method includes creating the secure association, and wherein creating a secure association includes the first network device:

obtaining discovery information from the second network device, the discovery information reflecting capabilities of the second network device to facilitate communication between with the first network device and the network;

authenticating the second network device;

sending a discovery verification request to the second network device for the discovery information of the second network device to be verified; and

receiving an acknowledgement receipt from the second network device verifying the discovery information.

35. (Original) A computer program product for use in a first network device that is engaged in a secure association with a second network device in a communications network, the computer program product comprising computer-executable instructions for implementing a method for verifying management frames transmitted between the network devices, the method comprising:

at the first network device creating a management frame configured to control the secure association;

at the first network device attaching a verifiable key to the management frame; and

at the first network device sending the management frame with the verifiable key to the second network device, wherein upon receiving the management frame and the verifiable key, the second network device recognizes the verifiable key and verifies the management frame prior to executing the management frame.

36. (Original) A computer program product as recited in claim 35, wherein at least one of the first and second network devices is a station configured to access the network and wherein at least one of the first and second network devices is an access point configured to provide the station access to the communications network.

37. (Original) A computer program product as recited in claim 36, wherein the first network device is a mobile and wireless communications device.

38. (Original) A computer program product as recited in claim 35, wherein the verifiable key is a provided by a server of the communications network.

39. (Original) A computer program product as recited in claim 35, wherein the verifiable key comprises a derivative of a key formed during authentication of at least one of the first and second network devices.

40. (Original) A computer program product as recited in claim 35, wherein prior to sending the management frame, the method includes creating the secure association, and wherein creating the secure association includes the first network device:

obtaining discovery information from the second network device, the discovery information reflecting capabilities of the second network device to facilitate communication between with the first network device and the network;

authenticating the second network device;

sending a discovery verification request to the second network device for the discovery information of the second network device to be verified; and

receiving an acknowledgement receipt from the second network device verifying the discovery information.